

INTERNATIONAL PERSPECTIVES ON CRYPTOGRAPHY POLICY: A UK PERSPECTIVE

Nigel Hickson

Department of Trade and Industry, Policy for IT Security
151 Buckingham Palace Road, London SW1W 9SS, U.K.

The United Kingdom authorities have, in common with other administrations, been working for some time to develop policies, concerning the use of encryption, which balance the ever increasing industry requirements (for strong security) with national law enforcement needs. Our efforts have been intensified by the requirements of UK businesses to play a full role in the emerging information society, which include being able to take part in global electronic commerce.

After two years of discussion Government Ministers have now committed themselves to an encryption policy which has, as its centre-piece, the licensing of Trusted Third Parties (TTPs) who will enable their clients (individuals or business) to have access to a number of different cryptographic services. The formal announcement, to Parliament, by the Science and Technology Minister, Ian Taylor, is given below. The most important service a TTP can offer, will, we believe, be integrity. An infrastructure whereby the public encryption keys of business can be verified and authenticated is urgently required to enable business to engage in commerce with companies with a degree of trust. In this context we hope that digital signatures will be one of the services a TTP may be able to offer. We also recognise that confidentiality, of both stored information and that which is transmitted, is becoming increasingly important for business. We therefore envisage that the TTPs will, in conjunction with IT suppliers, offer a key escrow service to allow their clients to converse securely with all other TTP clients on the "network". For law enforcement the TTPs - which will be licensed by Government - will be required to supply their client's private encryption keys to Government under due legal process. Apart from the latter there will be no new controls on the right of any company or individual to use encryption technologies in the UK.

There is, however, little point in establishing TTP networks solely in the UK. The needs of business (nor the communication networks to support them) are not restrained by national borders, and therefore to facilitate global commerce the "network" of TTPs (briefly referred to above) will need to be established. This will take time, will involve much policy discussion in the EU, OECD and other bodies, and will only happen if business wants it to. The UK have but taken a small first step.

**ENCRYPTION POLICY ANNOUNCEMENT:
PARLIAMENTARY ANSWER ON 10 JUNE 96**

Ian Taylor MP, Minister for Science and Technology

Following the discussion between Departments to which I referred in my replies to the hon Member for Brigg and Cleethorpes of 6 and 25 March, I am today publishing a paper outlining the Government's policy on the provision of encryption services on public networks. Copies of the paper are available in the library of both Houses.

The Government aims to facilitate the development of electronic commerce on the emerging global information infrastructure. This is of significant importance in maintaining the UK's competitiveness and is a component of the department's information society initiative. There is a growing demand for encryption services to safeguard the integrity and confidentiality of electronic

information transmitted on public telecommunications networks. The Government therefore proposes to make arrangements for licensing Trusted Third Parties (TTPs) who would provide such services. These TTPs would offer digital signature, data integrity and retrieval, key management and other services for which there is a commercial demand. The Licensing policy will aim to protect consumers as well as to preserve the ability of the intelligence and law enforcement agencies to fight serious crime and terrorism by establishing procedures for disclosure to them of the encryption keys, under safeguards similar to those which already exist for warranted interception under the Interception of Communications Act.

Officials from within my department have held preliminary discussions with industry groups on the concepts set out in the paper. The Government intends to bring forward proposals for legislation following consultation by the Department of Trade and Industry on detailed policy proposals.